(19) JAPANESE PATENT OFFICE

JPA11-338825

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11338825 A**

(43) Date of publication of application: **10.12.99**

(51) Int. Cl **G06F 15/00**
G06F 12/14
G06F 17/30
G09C 1/00
H04L 9/32

(21) Application number: **10148176**

(22) Date of filing: **29.05.98**

(71) Applicant: **HITACHI LTD**

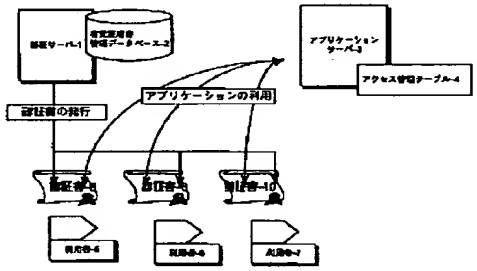
(72) Inventor: **MATSUNAGA KAZUO**

(54) **ACCESS CONTROL METHOD CONSIDERING CONFIGURATION OF ORGANIZATION**

(57) Abstract:

PROBLEM TO BE SOLVED: To attain access control to an application with reflection of a user and the configuration of organization by preparing a step where the access control is executed, based on the user organization information, by making reference to the access management information and in consideration of the assignment/organization configuration concerning the user.

SOLUTION: A user 5 accesses an application server 3 with addition of an authentication form 8 to use the service of the server 3. The server 3 authenticates the access authorization of the user 5, based on the form 8, and by making reference to an access management table 4 and then provides its service to the user 5 only when his access authorization is accepted. In such a constitution, the access control is attained to an application where the user 5 and the configuration of organization are reflected by means of the table 4 where an access authorization rule is defined and then the application load can be reduced without using an exclusive access server nor a DB which manages the total configuration of organization.



JPA11-338825

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－338825

(43)公開日　平成11年(1999)12月10日

(51)Int.Cl.[6]	識別記号	F I		
G06F 15/00	330	G06F 15/00	330	D
12/14	310	12/14	310	K
17/30		G09C 1/00	640	Z
G09C 1/00	640	G06F 15/40	320	B
H04L 9/32		H04L 9/00	671	

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平10－148176

(22)出願日　平成10年(1998)５月29日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　松永　和男
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

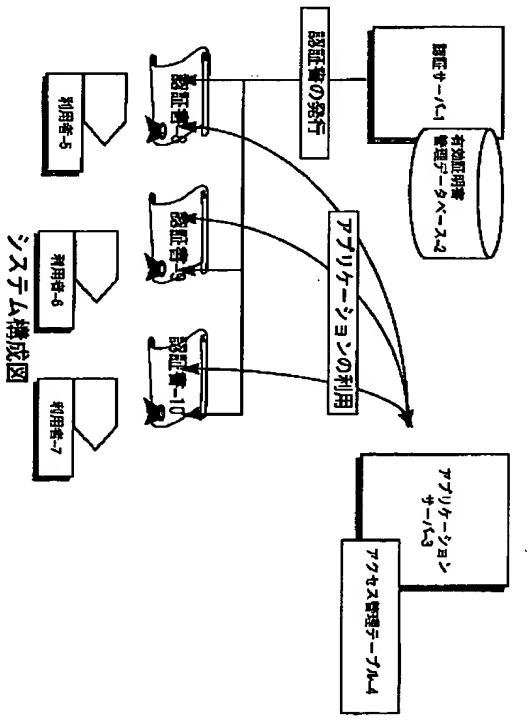
(74)代理人　弁理士　矢島　保夫

(54)【発明の名称】組織構成を考慮したアクセス制御方法

(57)【要約】

【課題】従来は、各アプリケーションが利用者全員の権限を管理したり、組織構成全体を管理するようなＤＢを設ける必要があり、職制変更等においてアプリケーションに格納された情報の変更等が大きな負担となっていた。本発明は、専用のアクセスサーバを必要とせず、かつ各アプリケーションが利用者全員の権限を管理したり、組織構成全体を管理するようなＤＢを設けることなく、アクセス権限のルールを定義したアクセス管理テーブルにより利用者及び組織構成を反映したアプリケーションに対するアクセス制御を実現することを目的とする。

【解決手段】利用者各個人に発行する認証書に組織構成を含む情報を付加することにより、アクセス要求を受けたアプリケーションは、利用者に与えられたアクセス権限に加えて、組織に与えられたアクセス権限を用いてアクセス制御を行う。組織に与えられたアクセス権限情報は、アクセス管理テーブルに格納され、利用者がアクセス要求を実行する毎に権限チェックを行うことで実現する。



1

【特許請求の範囲】
【請求項１】各利用者に対して、その利用者がアプリケーションを利用する際に必要な認証書であって、その利用者が属する組織に関する組織情報を格納した認証書を、発行するステップと、
アプリケーションに、所属または役職に対して許可される権限を定義するアクセス管理情報を用意しておくステップと、
アプリケーション利用時は、利用者から送られてくる認証書に格納された利用者の組織情報に基づき、上記アクセス管理情報を参照して、当該利用者に関する所属・組織構成を考慮したアクセス制御を実行するステップとを備えたことを特徴とするアクセス制御方法。
【請求項２】前記アクセス管理情報に、前記認証書に格納された組織情報とその利用者に付与するアクセス権限範囲をルール化したルールベースを、付加しておき、アクセス制御時には、該ルールベースを参照して利用者に関する所属・組織構成を考慮したアクセス制御を実行する請求項１に記載のアクセス制御方法。
【請求項３】有効な認証書を管理する認証書管理データベースを設け、アクセス権限チェック時に利用者の使用している認証書が有効であることを確認する請求項１に記載のアクセス制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、利用時にアクセス制御を必要とするアプリケーションを利用する場合に、アクセスする権限が組織構成にも依存して変化するアプリケーションのアクセス制御方法に関する。
【０００２】
【従来の技術】従来より、認証書を利用して個人を認証するアクセス制御方式が知られている。一方、例えば、会社組織の場合に、課長以上が参照可能なＤＢ等、個人毎でなく、組織に依存したアクセス制御を行いたい場合がある。このような組織を意識したアクセス制御を行う場合には、アプリケーションを実現するサーバと別にアクセス制御を専門に実行するアクセスサーバを用意し、アクセスサーバ内に組織構成を登録したＤＢ（データベース）を設け、アプリケーションにアクセスする場合には、一度アクセスサーバに権限があるかを問い合わせて許可、非許可を、各アプリケーションに通知していた。または、各アプリケーションが、利用者個人とその個人の組織における所属・役職を関連づける情報を保持することにより実現していた。すなわち、例えば利用者を識別する情報と権限（資格）を対応づけるファイル（ＤＢ）を使用することにより、アクセス権の管理を行うのが一般的であった。
【０００３】
【発明が解決しようとする課題】上記従来方式では、専用のアクセスサーバを用意したり、各アプリケーション

2

が利用者全員の権限を管理し組織構成全体を管理するようなＤＢを用意する必要がある。企業のように階層的な組織をとる場合に、慣習的に行われている職制の上位者が下位者の権限を包含する運用、また不在時の代行処理等を行うような運用等、利用形態に応じてカスタマイズすることで柔軟な運用を実現したいという要求があるが、上記従来技術ではそのような要求に応えるためには、専用のアクセスサーバを用意したり、各アプリケーションが利用者全員の権限を管理し組織構成全体を管理するようなＤＢを用意しなければならない。更に、職制の変更等により利用権限に変更が発生した場合、即時に変更後の権限での運用を可能としたいところであるが、上記従来技術ではそのような利用権限の変更も面倒である。
【０００４】本発明は、上述の従来方式における問題点に鑑み、専用のアクセスサーバを必要とせず、かつ各アプリケーションが利用者全員の権限を管理したり、組織構成全体を管理するようなＤＢを設けることなく、アクセス権限のルールを定義したアクセス管理テーブルにより利用者及び組織構成を反映したアプリケーションに対するアクセス制御を実現することを目的とする。また、階層的な組織における各種の利用形態に応じた柔軟な運用を行なうことができるアクセス制御を実現することを目的とする。更に、職制の変更等により利用権限に変更が発生した場合にも即時に変更後の権限での運用を可能とするアクセス制御を実現することを目的とする。
【０００５】
【課題を解決するための手段】上記目的を達成するため、本発明は、利用者各個人に発行する認証書に組織構成を含む情報を付加することにより、アクセス要求を受けたアプリケーションは利用者に与えられたアクセス権限に加えて組織に与えられたアクセス権限を用いてアクセス制御を行うことを特徴とする。組織に与えられたアクセス権限情報は、アクセス管理テーブルに格納され、利用者がアクセス要求を実行する毎に権限チェックを行うことで実現する。
【０００６】また、ルールベースにアクセス権限のルールを定義することで、アクセス管理テーブルに格納されたアクセス権限情報に加えて、ルールに定義されたアクセス制御を実現する。さらに、有効認証書管理データベースを設け、利用者がアクセス要求を実行する毎に認証書の有効性のチェックを行うことで、無効となった認証書によるアクセスを即時に禁止することを実現する。
【０００７】
【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。
【０００８】図１は、本発明の実施の形態のシステム全体の構成図を示す。認証サーバ１は利用者５、６、７全員に対して、あらかじめ認証書８、９、１０をそれぞれ発行しておく。また、有効な認証書を管理するための有

効証明書管理データベース２に、発行した認証書を登録しておく。

【０００９】例えば、利用者５は、アプリケーションサーバ３のサービスを利用する場合に、認証書８を添付してアクセスする。アプリケーションサーバ３は、添付された認証書８を用いて、かつアクセス管理テーブル４（後述する）を参照することで、利用者５のアクセス権限を確認し、許可される場合のみサービスを提供する。図２は、アプリケーションの利用者に認証書を発行する処理を示す。認証書は、組織の利用者全員に個人毎に発行する。認証書には、組織を示す情報を格納する（図３で後述）。職制の変更等により、組織を示す情報に変更が発生する場合には、改めて認証サーバ１から、変更となった各利用者に対して認証書を発行する。新たに認証書を発行した場合、認証サーバ１は、有効証明書管理データベース２にその認証書を登録する。また、組織の変更により従来使用していた認証書を無効化するために、有効証明書管理データベース２から、無効とすべき認証書を削除する。

【００１０】図３は、認証サーバ２が発行する認証書１１の形式を示している。認証サーバ１が発行する認証書１１は、X.509勧告に準拠する形式であり、基本部分１２と拡張部分１３とから成る。基本部分１２は、X.509により規定された形式で必要な情報を格納する。拡張部分１３は、利用者が独自に形式を規定できる部分であり、ここに組織を表す情報を格納する。

【００１１】図４は、アプリケーションの例として、掲示板機能を実現するデータベース１４のアクセス管理テーブル１５の例を示す。このデータベース１４のアクセス管理テーブル１５には、掲示板情報として格納されている情報毎にアクセス管理する対象者の権限定義と、付与する権限を一覧にして格納してある。権限定義は、個人の組織情報であり、例えば所属または役職を列挙する。権限は、権限定義した対象者のアクセス権限を示す部分であり、例えば、掲示板情報を参照可能かまたは更新まで可能かなどを設定する。このようなアクセス管理テーブルが、各アプリケーションに対応して設けられている。

【００１２】図５は、掲示板を利用するときのアクセス制御の例である。利用者５は、あらかじめ個人毎の認証書１７を保持しておき、掲示板サーバ１６を参照するときに参照要求１８と共に、個人の認証書１７を掲示板サーバ１６に送信する。要求を受け付けた掲示板サーバ１６は、認証書１７に格納された個人の所属・役職等を取り出し、掲示情報データベース１４のアクセス管理テーブル１５を参照し、利用者が要求している情報がアクセス許可されているかチェックし、許可されていなければ参照不可１９により拒否し、許可されていれば要求された情報(人事情報転送２０)を転送する。

【００１３】図６は、ルールを用いてアクセス制御権限を定義する例である。掲示情報データベース１４のアクセス管理テーブル１５に加えて、各種の情報に共通的なアクセスルールをルールベース２１として作成しておく。そして、アクセス権限のチェックを行うとき、このルールにしたがって許可できるか否か判定する。例えば、組織構成の上位者は下位者のアクセス権限を包含するルールを作成すると、本部長は副本部長に与えられたアクセス権限を持つことになる。本例では、他事業所予算について、副本部長に参照権限が与えられているが、ルール１があることから本部長も参照権限を持つことになる。同様に、部長間の代行処理を実現するためには、部長名を特定して代行関係をルールベース２１に定義することで実現可能となる。本例では、Ａ部長はＢ部長の代行を可能と定義しているため、Ａ部長はＢ部の勤休ＤＢを更新可能となる。

【００１４】図７は、有効認証書管理データベース２２を利用することにより、所属・組織の変更があった場合に、変更前に発行した認証書を即時に利用不可とすることを可能とする例である。有効認証書管理データベース２２には、認証サーバ１の発行した有効な認証書のみを格納する。掲示板サーバ１６は、アクセス権限チェック２３を行うときに、利用者の使用している認証書が有効であることを有効認証書管理データベース２２を参照して確認する。これにより有効な認証書のみによるアクセスを実現することができる。

【００１５】

【発明の効果】以上説明したように、本発明によれば、専用のアクセスサーバを必要とせず、かつ各アプリケーションが利用者全員の権限を管理したり、組織構成全体を管理するようなＤＢを設けることなく、アクセス権限のルールを定義したアクセス管理テーブルにより利用者及び組織構成を反映したアプリケーションに対するアクセス制御を実現し、アプリケーションの負荷を軽減することができる。また、階層的な組織における各種の利用形態に応じた柔軟な運用を行なうことができるアクセス制御を実現できる。さらに、利用者の所属・組織の変更があった場合に、変更前に発行した認証書を即時に利用不可とすることができる。アクセス管理テーブルやルールのカスタマイズは容易であるので、多様な運用を可能とできる。

【図面の簡単な説明】

【図１】本発明の実施の形態のシステム全体の構成図

【図２】利用者に認証書を発行する処理を示す図

【図３】認証サーバが発行する認証書の形式を示す図

【図４】掲示板機能を実現するデータベースのアクセス管理テーブルの例を示す図

【図５】掲示板を利用するときのアクセス制御の例を示す図

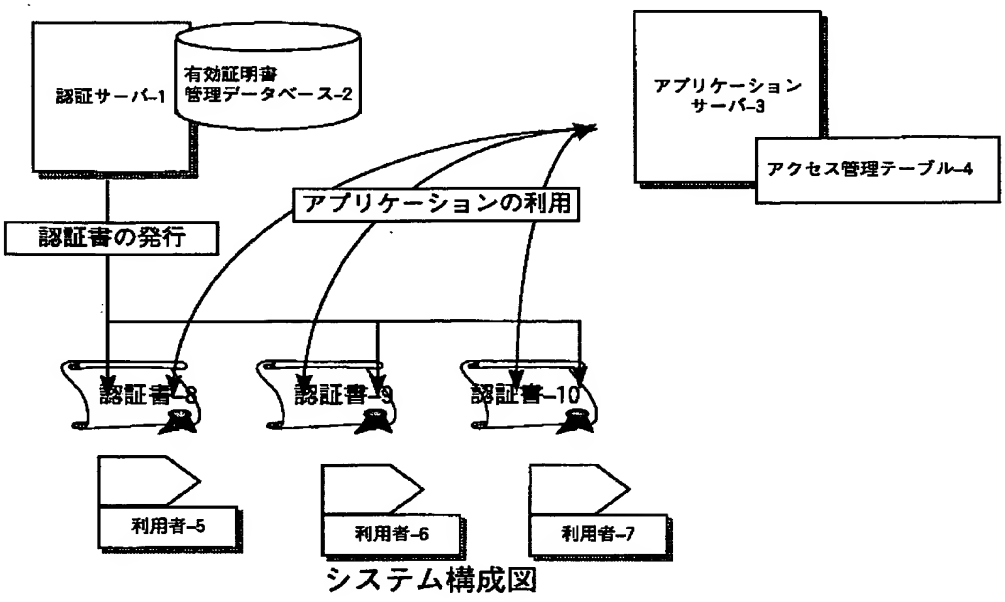
【図６】ルールを用いてアクセス制御権限を定義する例を示す図

【図７】所属・組織の変更があった場合に、変更前に発行した認証書を即時に利用不可とすることを可能とする例を示す図

【符号の説明】

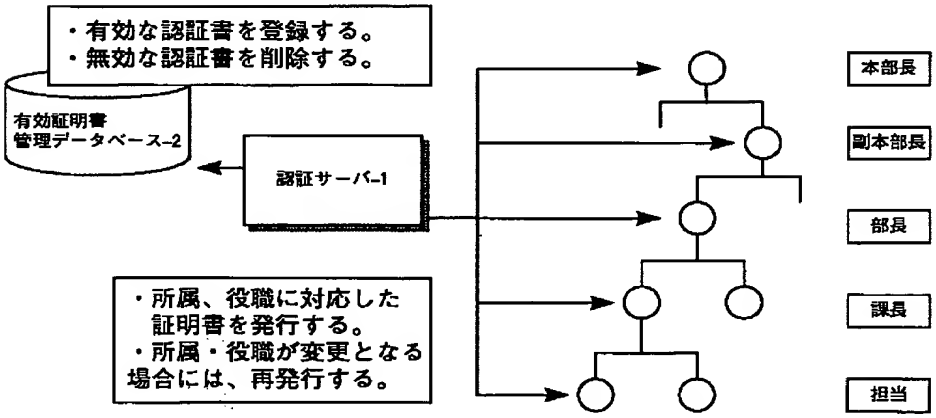
１…認証サーバ、２…有効証明書管理データベース、３…アプリケーションサーバ、４…アクセス管理テーブル、５～７…利用者、８～１０…認証書。

【図１】



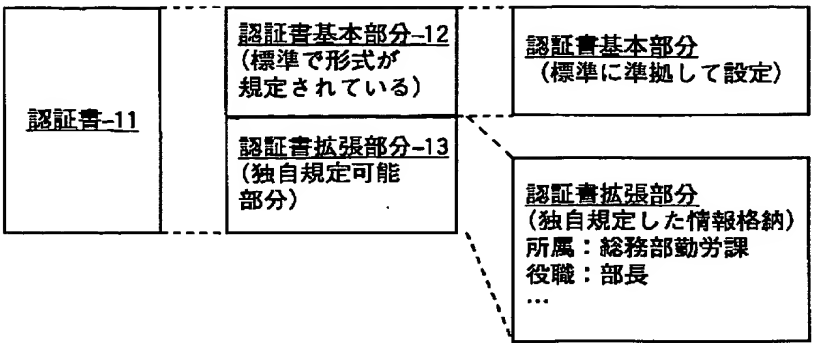
システム構成図

【図２】



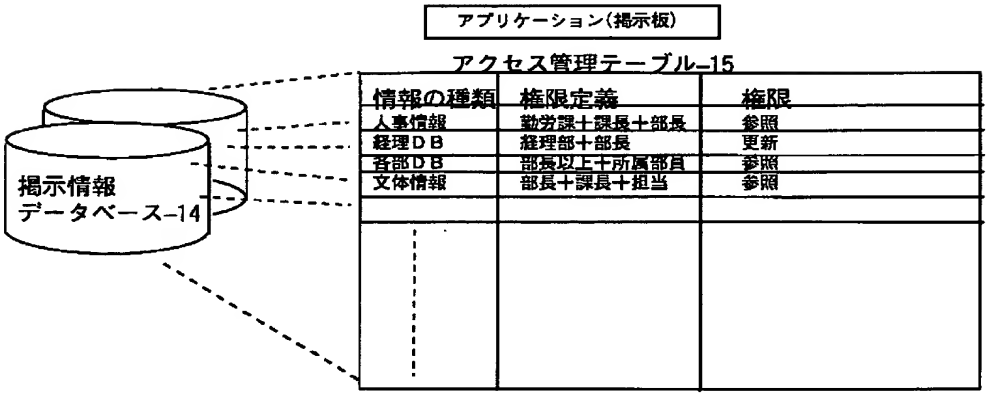
個人への認証書の発行

【図３】



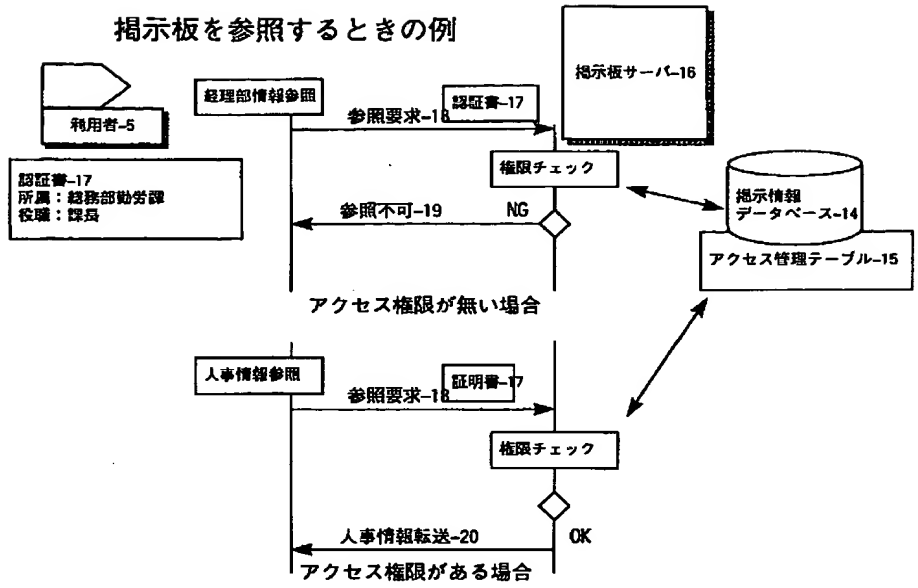
認証書フォーマット例

【図４】

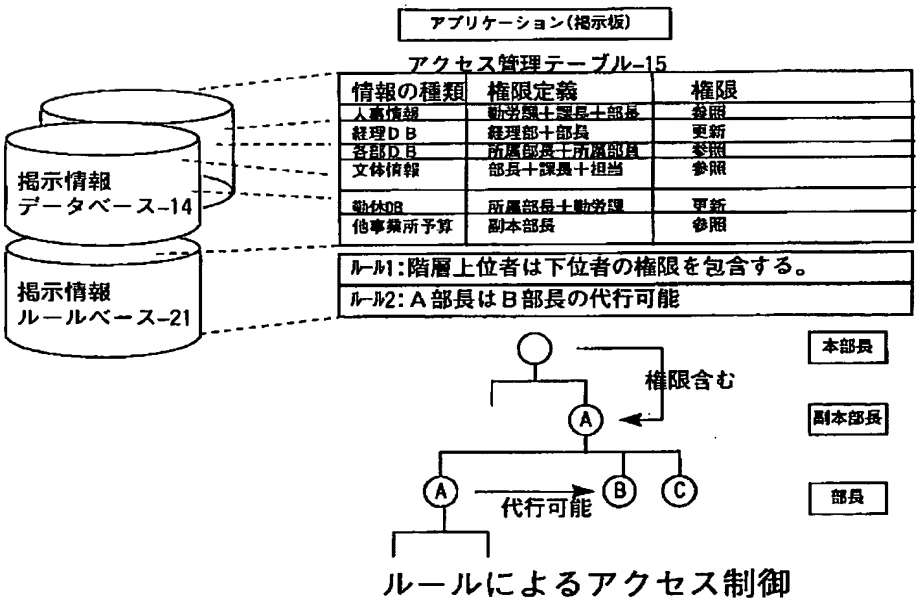


データベースのアクセス管理テーブル

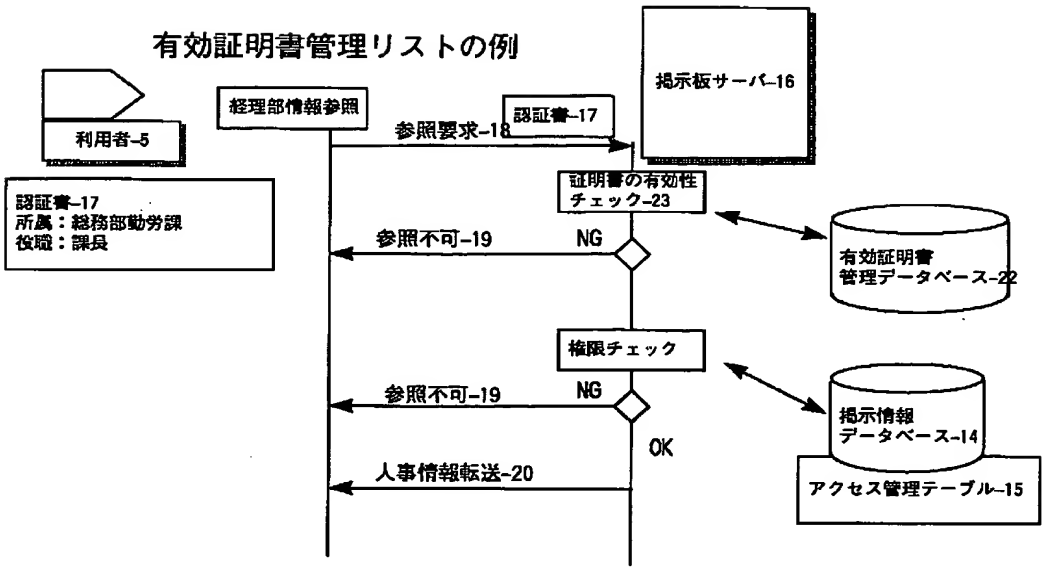
【図５】


掲示板を参照するときの例
掲示板サーバ-16
経理部情報参照
認証書-17
参照要求-18
利用者-5
認証書-17
所属：総務部勤労課
役職：課長
権限チェック
掲示情報
データベース-14
参照不可-19
NG
アクセス管理テーブル-15
アクセス権限が無い場合
人事情報参照
証明書-17
参照要求-18
権限チェック
人事情報転送-20
OK
アクセス権限がある場合

【図６】


アプリケーション(掲示板)
アクセス管理テーブル-15
情報の種類
権限定義
権限
人事情報
勤労課＋課長＋部長
参照
経理ＤＢ
経理部＋部長
更新
各部ＤＢ
所属部長＋所属部員
参照
文体情報
部長＋課長＋担当
参照
勤休DB
所属部長＋勤労課
更新
他事業所予算
副本部長
参照
掲示情報
データベース-14
掲示情報
ルールベース-21
ルール1:階層上位者は下位者の権限を包含する。
ルール2:Ａ部長はＢ部長の代行可能
本部長
権限含む
副本部長
A
A
B
C
代行可能
部長
ルールによるアクセス制御

【図７】



フロントページの続き

(51)Int.Cl.[6]	識別記号	ＦＩ
		Ｈ０４Ｌ　9/00　　６７５Ｄ